

Complete permutation polynomials from exceptional polynomials

D. Bartoli, M. Giulietti, L. Quoos, and G. Zini

Abstract

We classify complete permutation monomials of degree $\frac{q^n-1}{q-1} + 1$ over the finite field with q^n elements, for $n+1$ a prime and $(n+1)^4 < q$. As a corollary, a conjecture by Wu, Li, Helleseht, and Zhang is proven. When $n+1$ is a power of the characteristic we provide some new examples. Indecomposable exceptional polynomials of degree 8 and 9 are also classified.

Keywords: Permutation polynomials, complete permutation polynomials, exceptional polynomials, bent-negabent boolean functions.

1 Introduction

Let \mathbb{F}_ℓ denote the finite field of order ℓ and characteristic p . A *permutation polynomial* (or PP) $f(x) \in \mathbb{F}_\ell[x]$ is a bijection of \mathbb{F}_ℓ onto itself. If $f(x) \in \mathbb{F}_\ell$ is a permutation polynomial over \mathbb{F}_{ℓ^m} for infinitely many m , then $f(x)$ is said to be an *exceptional polynomial* over \mathbb{F}_ℓ . A polynomial $f(x) \in \mathbb{F}_\ell[x]$ is a *complete permutation polynomial* (or CPP) of \mathbb{F}_ℓ if both $f(x)$ and $f(x) + x$ are permutation polynomials of \mathbb{F}_ℓ .

CPPs are also related to bent and negabent functions which are studied for a number of applications in cryptography, combinatorial designs, and coding theory; see for instance [6, 11, 15, 20].

The most studied class of CPPs is the monomial one. If there exists a complete permutation monomial of degree d over \mathbb{F}_ℓ , then d is called a CPP exponent over \mathbb{F}_ℓ . Complete permutation monomials have been investigated in a number of recent papers, especially for $\ell = q^n$ and $d = \frac{\ell-1}{q-1} + 1$. Note that for an element $\alpha \in \mathbb{F}_\ell^*$, the monomial αx^d is a CPP of \mathbb{F}_ℓ if and only if $\gcd(d, \ell-1) = 1$ and $\alpha x^d + x$ is a PP of \mathbb{F}_ℓ . In [2, 3, 16, 17] PPs of type $f_b(x) = x^{\frac{q^n-1}{q-1}+1} + bx$ over \mathbb{F}_{q^n} are thoroughly investigated for $n = 2$, $n = 3$, and $n = 4$. For $n = 6$, sufficient conditions for f_b to be a PP of \mathbb{F}_{q^6} are provided in [16, 17] in the special

cases of characteristic $p \in \{2, 3, 5\}$, whereas in [1] all a 's for which $ax^{\frac{q^6-1}{q-1}+1}$ is a CPP over \mathbb{F}_{q^6} are explicitly listed. The case $p = n + 1$ is dealt with in [13].

In this paper we discuss monomials of degree $d = \frac{q^n-1}{q-1} + 1$ for general n . The starting point of our investigation is the observation that $b^{-1}x^d \in \mathbb{F}_{q^n}[x]$ is a CPP of \mathbb{F}_{q^n} if and only if $b, b^q, \dots, b^{q^{n-1}}$ are the roots of

$$v_g(x) = \frac{g(-x) - g(0)}{-x} \in \mathbb{F}_q[x]$$

for some permutation polynomial $g(x)$ of degree $n+1$ over \mathbb{F}_q such that the first-degree term is not zero. If for a root b of $v_g(x)$ the monomial $b^{-1}x^d$ is a CPP over \mathbb{F}_{q^n} , then $g(x)$ will be called a *good* PP over \mathbb{F}_q ; in this case, all roots of $v_g(x)$ have the same property. Clearly, a PP $g(x)$ over \mathbb{F}_q is good if and only if the roots of $v_g(x)$ in the algebraic closure of \mathbb{F}_q form a unique orbit under the action of the Frobenius map $x \mapsto x^q$.

Our aim is to classify good permutation polynomials over \mathbb{F}_q . Here we achieve this goal for all n , $(n+1)^4 < q$, with the exception of the cases $n+1 = p^r$, with $r > 1$, and $n+1 = p^r(p^r-1)/2$, with $p \in \{2, 3\}$. For $n+1 = p^r$ we provide several examples. Proposition 3.4 shows that, if $q = p^k$ and $n+1$ is a prime different from p satisfying $\gcd(n, k) = \gcd(n+1, p^2-1) = 1$, then $d = \frac{q^n-1}{q-1} + 1$ is a CPP exponent over \mathbb{F}_{q^n} . This solves a conjecture by Wu, Li, Helleseht, and Zhang, see [17, Conjecture 4.18 and Proposition 4.19]. Our classification implies a result by Bhattacharya and Sarkar (see [5, Theorem 1.1]) which determines the PPs of type f_b when $p = 2$, n is a power of 2, and $b \in \mathbb{F}_{q^2}$.

Note that since every permutation polynomial with degree less than $q^{1/4}$ is exceptional (see [14, Theorem 8.4.19]), condition $(n+1)^4 < q$ allows us to consider only exceptional polynomials. A key tool in our investigation is the classification of indecomposable exceptional polynomials of degree different from p^r for some $r > 1$; see [14, Section 8.4].

If $g(x)$ is a good PP over \mathbb{F}_q then it is easily seen that $c \cdot g(c'x) + e$ is a good PP over \mathbb{F}_q for each $c, c', e \in \mathbb{F}_q$ with $cc' \neq 0$. In this paper two PPs $g(x)$ and $h(x)$ over \mathbb{F}_q will be called *CPP-equivalent* if there exist $c, c', e \in \mathbb{F}_q$ with $cc' \neq 0$ such that $h(x) = c \cdot g(c'x) + e$. Note that for $g(x)$ a PP over \mathbb{F}_q and $k \in \mathbb{F}_q$, the permutation polynomials $g(x+k)$ and $g(x)$ are equivalent in the usual sense but not CPP-equivalent; in fact, it's possible that one of them is good but the other is not. Note that, when $g'(x)$ ranges over the CPP-equivalence class of $g(x)$, the roots of $v_{g'}(x)$ range over the roots of $v_g(x)$ and their multiples by non-zero elements in \mathbb{F}_q . We will consider only one polynomial in a CPP-equivalence class. In particular, we assume that $g(x)$ is monic and that $g(0) = 0$. Since exceptional polynomials only exist for degrees coprime with $q-1$, when n is odd we assume that $p = 2$.

Our first result is that if g is decomposable, that is g is a composition of two exceptional polynomials with degree greater than one, then g is not good; see Proposition 2.4.

If $g(x) \in \mathbb{F}_q[x]$ is a monic indecomposable exceptional polynomial of degree $n+1$ with $g(0) = 0$, then, up to CPP-equivalence, one of the following holds [14, Section 8.4].

A) $n + 1$ is a prime different from p not dividing $q - 1$, and

A1) $g(x) = (x + e)^{n+1} - e^{n+1}$, with $e \in \mathbb{F}_q$, or

A2) $g(x) = D_{n+1}(x + e, a) - D_{n+1}(e, a)$, where $a, e \in \mathbb{F}_q$, $a \neq 0$, $n + 1 \nmid q^2 - 1$, and $D_{n+1}(x, a)$ denotes a Dickson polynomial of degree $n + 1$.

B) $n + 1 = p$ and $g(x) = (x + e)((x + e)^{\frac{p-1}{r}} - a)^r - e(e^{\frac{p-1}{r}} - a)^r$, with $r \mid p - 1$, $a, e \in \mathbb{F}_q$, and $a^{r(q-1)/(p-1)} \neq 1$.

C) $n + 1 = s(s - 1)/2$, where $p \in \{2, 3\}$, $q = p^m$, $s = p^r > 3$, and $(r, 2m) = 1$.

D) $n + 1 = p^r$ with $r > 1$.

For the case $n + 1 = p^r$, $r > 1$, Guralnick and Zieve conjectured in [10] that there are no examples of indecomposable exceptional polynomials other than those described in [14, Propositions 8.4.15, 8.4.16, 8.4.17].

The paper is organized as follows. We classify good exceptional polynomials of type A) and B) in Sections 3 and 4; see Theorems 3.1 and 4.1. We show in Section 5 that certain exceptional polynomials of type C) are not good; see Proposition 5.1. We describe in Section 6 some good exceptional polynomials of type D); see Propositions 6.1, 6.2, and 6.3. Finally, we determine all the exceptional polynomials of degree 8 and 9 (see Propositions 7.1 and 7.5); in this way we provide a proof of the above mentioned Guralnick-Zieve conjecture for the special cases $n = 7, 8$. As a byproduct, we obtain all the CPPs with $n + 1 = 8$ and $n + 1 = 9$; see Corollaries 7.4 and 7.9 in Section 7.

2 Preliminaries

Throughout the paper, q will be a power p^m of a prime p and ζ_s will denote a s -th primitive root of unity, for $s \geq 1$. We begin this section by rephrasing a result by Wu, Li, Helleseeth, and Zhang [18]. For $b \in \mathbb{F}_{q^n}$, let $A_i(b) \in \mathbb{F}_q$ denote the evaluation of the i -th elementary symmetrical polynomial in $b, b^q, \dots, b^{q^{n-1}}$, that is,

$$A_i(b) = \sum_{0 \leq j_1 < j_2 < \dots < j_i \leq n-1} b^{q^{j_1} + q^{j_2} + \dots + q^{j_i}}.$$

As a matter of notation let $A_0(b) = 1$. Recall that $b, b^q, \dots, b^{q^{n-1}}$ are the roots of the polynomial

$$(-1)^n A_n(b) + (-1)^{n-1} A_{n-1}(b)T + \dots + (-1)^{n-i} A_{n-i}(b)T^i + \dots + T^n.$$

By [18, Lemma 5] we have the following result.

Proposition 2.1. *Assume that $(n+1)^4 < q$. The monomial $b^{-1}x^{\frac{q^n-1}{q-1}+1}$ is a CPP over \mathbb{F}_{q^n} if and only if $\gcd(n+1, q-1) = 1$ and $\sum_{i=0}^n A_{n-i}(b)x^{i+1}$ is an exceptional polynomial over \mathbb{F}_q .*

Let $g(x) = \sum_{i=0}^{n+1} \lambda_{n+1-i}x^i$ be an exceptional polynomial over \mathbb{F}_q , and assume that $\lambda_n \neq 0$ and $\lambda_0 = 1$. Consider the polynomial

$$h_g(x) = \frac{g(x) - g(0)}{x} = \frac{\sum_{i=1}^{n+1} \lambda_{n+1-i}x^i}{x} = \sum_{i=0}^n \lambda_{n-i}x^i.$$

Then $v_g(x) := h_g(-x) = \sum_{i=0}^n (-1)^i \lambda_{n-i}x^i$. Note that if n is even, then $h_g(-x)$ can be written as $\sum_{i=0}^n (-1)^{n-i} \lambda_{n-i}x^i$. If n is odd, then $p = 2$ and the same relation holds.

This means that, for any root b of $v_g(x)$, the monomial $b^{-1}x^{\frac{q^n-1}{q-1}+1}$ is a CPP over \mathbb{F}_{q^n} if and only if the roots of $v_g(x)$, or equivalently $h_g(-x)$, form a unique orbit under the Frobenius map $x \mapsto x^q$. This motivates the following definition.

Definition 2.2. *An exceptional polynomial $g(x) \in \mathbb{F}_q[x]$ with $g(0) = 0$ and $g'(0) \neq 0$ is said to be good if the roots of $\frac{g(-x)}{-x}$ form a unique orbit under the Frobenius map $x \mapsto x^q$.*

Therefore, the following has been proved.

Proposition 2.3. *Assume that $(n+1)^4 < q$. Then the elements $b \in \mathbb{F}_{q^n} \setminus \mathbb{F}_q$ such that $b^{-1}x^{\frac{q^n-1}{q-1}+1}$ is a CPP over \mathbb{F}_{q^n} are the roots of polynomials $\frac{g(-x)}{-x}$, for g ranging over good exceptional polynomials of degree $n+1$ over \mathbb{F}_q , with $g(0) = 0$ and $g'(0) \neq 0$.*

Note that $h_g(x)$ can be viewed as the bivariate polynomial $\frac{g(x)-g(y)}{x-y}$ evaluated at $y = 0$. So, assume that we know the factorization of $\frac{g(x)-g(y)}{x-y}$ into absolutely irreducible factors defined over the algebraic closure of \mathbb{F}_q , say $\frac{g(x)-g(y)}{x-y} = \prod_{k=1}^s \ell_k(x, y)$. Then

$$h_g(x) = \prod_{k=1}^s \ell_k(x, 0).$$

Obviously, this can be extremely useful to establish whether an exceptional polynomial g is good or not. Recall that an exceptional polynomial $g(t)$ is decomposable if there exist exceptional polynomials g_1, g_2 with degree greater than 1 such that $g(x) = g_1(g_2(x))$.

Proposition 2.4. *If $g(x)$ is a good exceptional polynomial, then $g(x)$ is not decomposable.*

Proof. Suppose that $g(x)$ is decomposable and write $g(x) = g_1(g_2(x))$, with polynomials g_1, g_2 such that $\deg(g_1), \deg(g_2) > 1$. Then

$$v_g(x) = \frac{g_1(g_2(-x)) - g_1(g_2(0))}{-x} = \frac{g_2(-x) - g_2(0)}{-x} \lambda(g_2(-x)),$$

with

$$\lambda(g_2(-x)) = \prod_{i=1}^{\deg(g_1)-1} (g_2(-x) - \beta_i)$$

for some $\beta_i \in \overline{\mathbb{F}}_q$. Since $\frac{g_2(-x)-g_2(0)}{-x}$ is a factor of positive degree defined over \mathbb{F}_q , the only possibility for the roots of $v_g(x)$ to form a unique orbit under the Frobenius map is that $v_g(x)$ is a power of $\frac{g_2(-x)-g_2(0)}{-x}$. Note that 0 cannot be a root of $v_g(x)$, since for $b = 0$ the monomial $bx^{\frac{q^n-1}{q-1}+1}$ is not a CPP. On the other hand, any root of a factor $g_2(-x) - \beta_i$ must be a root of $g_2(-x) - g_2(0)$, that is $\beta_i = g_2(0)$. Therefore,

$$v_g(x) = \left(\frac{g_2(-x) - g_2(0)}{-x} \right)^{\deg(g_1)} (-x)^{\deg(g_1)-1},$$

which is impossible since $\deg(g_1) > 1$. □

3 CPPs from exceptional polynomials of type A)

Throughout this section we assume that $n+1 \geq 3$ is a prime different from p . We denote by $T_{q^{n/2}}$ the absolute trace map $\mathbb{F}_{q^{n/2}} \rightarrow \mathbb{F}_2$, $x \mapsto x + x^2 + x^4 + \dots + x^{(q^{n/2})/2}$. We are going to prove the following result.

Theorem 3.1. *Assume that $(n+1)^4 < q$. For $i \in \{1, \dots, n/2\}$ let*

$$\alpha_i = \zeta_{n+1}^i + \zeta_{n+1}^{-i} \text{ and } \beta_i = \zeta_{n+1}^i - \zeta_{n+1}^{-i}.$$

Then the monomial $b^{-1}x^{\frac{q^n-1}{q-1}+1}$ is a CPP of \mathbb{F}_{q^n} precisely in the following cases.

- If $p \neq 2$:
 - i) *the order of q modulo $n+1$ is n and, up to multiplication by a non-zero element in \mathbb{F}_q , b is as follows:*
 - (a) $b = \zeta_{n+1}^i - 1$, for some $i \in \{1, \dots, n\}$;
 - (b) for $n/2$ even, $b = e(\alpha_i - 2) \pm \sqrt{\beta_i^2(e^2 - 4a)}$ for some $i \in \{1, \dots, n/2\}$, $a \in \mathbb{F}_q^*$, and $e \in \mathbb{F}_q$;
 - (c) for $n/2$ odd, $b = e(\alpha_i - 2) \pm \sqrt{\beta_i^2(e^2 - 4a)}$ for some $i \in \{1, \dots, n/2\}$, $a \in \mathbb{F}_q^*$, and $e \in \mathbb{F}_q$ such that $e^2 - 4a$ is a square in \mathbb{F}_q .
 - ii) *the order of q modulo $n+1$ is $n/2$, n is not divisible by 4, and, up to multiplication by a non-zero element in \mathbb{F}_q , $b = e(\alpha_i - 2) \pm \sqrt{\beta_i^2(e^2 - 4a)}$ for some $i \in \{1, \dots, n/2\}$, $a \in \mathbb{F}_q^*$, and $e \in \mathbb{F}_q$ such that $e^2 - 4a$ is 0 or a non-square in \mathbb{F}_q .*

- If $p = 2$:

- i) the order of q modulo $n + 1$ is n and, up to multiplication by a non-zero element in \mathbb{F}_q , $b = \zeta_{n+1}^i - 1$ for some $i \in \{1, \dots, n\}$;
- ii) the order of q modulo $n + 1$ is n or $n/2$, and

$$b = z_i := \varepsilon \delta_i^2 + (\varepsilon + \varepsilon^2) \delta_i^4 + \dots + (\varepsilon + \varepsilon^2 + \dots + \varepsilon^{q^n/4}) \delta_i^{q^n/2} \quad \text{or} \quad b = z_i + 1,$$

where $\varepsilon \in \mathbb{F}_{q^n}$ satisfies $T_{q^{n/2}}(\varepsilon) = 1$ and, for some $i \in \{1, \dots, n\}$, $\delta_i = \frac{1}{\alpha_i} + \frac{a}{e^2}$ and $T_{q^{n/2}}(\delta_i) = 1$.

By Propositions 2.1 and 2.4, the determination of the CPPs of type $b^{-1}x^{\frac{q^n-1}{q-1}+1}$ over \mathbb{F}_{q^n} relies on the classification of indecomposable exceptional polynomials, which is given in [14, Section 8.4]. In particular, by [14, Theorem 8.4.11], Theorem 3.1 is implied by the results of Sections 3.1 and 3.2.

3.1 CPPs from exceptional polynomials of type A1)

Throughout this subsection we also assume that $n + 1$ does not divide $q - 1$. Note that for each $e \neq 0$ the polynomial $g(x) = (x + e)^{n+1} - e^{n+1}$ has a non-zero term of degree one. Also, the n distinct roots of $h_g(-x) = \frac{(-x+e)^{n+1} - e^{n+1}}{-x}$ are

$$-e(\zeta_{n+1}^i - 1), \quad i = 1, \dots, n.$$

Proposition 3.2. *Assume that $e \in \mathbb{F}_q^*$. The polynomial $(x+e)^{n+1} - e^{n+1}$ is a good exceptional polynomial over \mathbb{F}_q if and only if the order of q modulo $n + 1$ is equal to n .*

Proof. The roots of $h_g(-x)$ form a unique orbit under the Frobenius map if and only if ζ_{n+1} does not belong to any proper subfield of \mathbb{F}_{q^n} . This is equivalent to the order of q modulo $n + 1$ being equal to n . \square

Corollary 3.3. *Assume that the order of q modulo $n + 1$ is equal to n . Then for $b = e(\zeta_{n+1}^i - 1)$ the monomial $b^{-1}x^{\frac{q^n-1}{q-1}+1}$ is a CPP of \mathbb{F}_{q^n} , for each $e \in \mathbb{F}_q^*$ and $i \in \{1, \dots, n\}$.*

3.2 CPPs from exceptional polynomials of type A2)

Throughout this subsection we further assume that $n + 1$ does not divide $q^2 - 1$. We begin by considering Dickson polynomials $D_{n+1}(x, a) \in \mathbb{F}_q[x]$. Recall that

$$D_{n+1}(x, a) = \sum_{k=0}^{n/2} \frac{n+1}{n+1-k} \binom{n+1-k}{k} (-a)^k x^{n+1-2k}.$$

Note that $D_{n+1}(x, a)$ has a non-zero term of degree 1, for each $a \neq 0$. In [4, Theorems 7 and 8] Bhargava and Zieve provide the factorization of $\frac{D_{n+1}(x+e, a) - D_{n+1}(y+e, a)}{x-y}$, $e \in \mathbb{F}_q$.

Proposition 3.4. *The polynomial $g(x) = D_{n+1}(x+e, a) - D_{n+1}(e, a)$, with $a, e \in \mathbb{F}_q$, $a \neq 0$, and $D'_{n+1}(e, a) \neq 0$, is a good exceptional polynomial over \mathbb{F}_q if and only if one of the following cases occurs:*

- i) $p \neq 2$, $n/2$ is even and the order of q modulo $n+1$ is n ;
- ii) $p \neq 2$, $n/2$ is odd and either $e^2 - 4a$ is 0 or a non-square in \mathbb{F}_q and the order of q modulo $n+1$ is $n/2$, or $e^2 - 4a$ is a square in \mathbb{F}_q and the order of q modulo $n+1$ is n ;
- iii) $p = 2$, the order of q modulo $n+1$ is n or $n/2$, and $T_{q^{n/2}}(\delta_1) = 1$, where $\delta_i = \frac{1}{\alpha_i} + \frac{a}{e^2}$.

In Cases i) and ii), the roots of $h_g(-x)$ are

$$b = -\frac{1}{2} \cdot \left(e(\alpha_i - 2) \pm \sqrt{\beta_i^2(e^2 - 4a)} \right).$$

In Case iii), let $\varepsilon \in \mathbb{F}_{q^n}$ with $T_{q^{n/2}}(\varepsilon) = 1$. Then the roots of $h_g(-x)$ are

$$b = \varepsilon \delta_i^2 + (\varepsilon + \varepsilon^2) \delta_i^4 + \dots + (\varepsilon + \varepsilon^2 + \dots + \varepsilon^{q^{n/4}}) \delta_i^{q^{n/2}} \quad \text{and} \quad b + 1.$$

Proof. By [4, Theorem 7] we have

$$D_{n+1}(x+e, a) - D_{n+1}(y+e, a) = (x-y) \prod_{i=1}^{n/2} ((x+e)^2 - \alpha_i(x+e)(y+e) + (y+e)^2 + \beta_i^2 a),$$

where $\alpha_i = \zeta_{n+1}^i + \zeta_{n+1}^{-i}$ and $\beta_i = \zeta_{n+1}^i - \zeta_{n+1}^{-i}$. Then

$$h_g(-x) = \frac{D_{n+1}(-x+e, a) - D_{n+1}(e, a)}{-x} = \prod_{i=1}^{n/2} ((-x+e)^2 - \alpha_i e(-x+e) + e^2 + \beta_i^2 a),$$

that is, since $\alpha_i^2 = \beta_i^2 + 4$,

$$h_g(-x) = \prod_{i=1}^{n/2} (x^2 + xe(\alpha_i - 2) + (\alpha_i - 2)((\alpha_i + 2)a - e^2)).$$

Note that the values $e(\alpha_i - 2)$ are pairwise distinct for $i = 1, \dots, n$; hence, the sets of roots of two distinct quadratic factors of $h_g(-x)$ are disjoint.

Assume $p \neq 2$. Since $\alpha_i^2 = \beta_i^2 + 4$, the roots of $h_g(-x)$ are

$$-\frac{1}{2} \cdot \left(e(\alpha_i - 2) \pm \sqrt{\beta_i^2(e^2 - 4a)} \right).$$

Since $(\beta_i^2(e^2 - 4a))^{q^j} = (\beta_{iq^j \pmod{n+1}})^2(e^2 - 4a)$, if the roots of $h_g(-x)$ form a unique orbit under the Frobenius map then the order $\text{ord}_{n+1}(q)$ of q in \mathbb{Z}_{n+1}^* must be either n or $n/2$.

Thus, we check when $\beta_i^2(e^2 - 4a)$ is a non-square in $\mathbb{F}_{q^{n/2}}$, so that the $(n/2)$ -th power of the Frobenius map permutes the roots of $h_g(-x)$. Note that if $\text{ord}_{n+1}(q) = n/2$, then $\beta_i^{q^{n/2}} = \beta_i$ and therefore β_i^2 is a square in $\mathbb{F}_{q^{n/2}}$; if on the contrary $\text{ord}_{n+1}(q) = n$, then $\beta_i^{q^{n/2}} = -\beta_i$ and β_i^2 is a non-square in $\mathbb{F}_{q^{n/2}}$. Also, $n/2$ even implies that $(e^2 - 4a)$ is always a square in $\mathbb{F}_{q^{n/2}}$, whereas if $n/2$ is odd then $(e^2 - 4a)$ is a square in $\mathbb{F}_{q^{n/2}}$ if and only if it is a square in \mathbb{F}_q .

If $e^2 - 4a = 0$, then $h_g(-x)$ is a square and its roots form a unique orbit under Frobenius. This completes the proof for $p \neq 2$.

For $p = 2$, similar computations using the solutions of quadratic equations in characteristic 2 provide the claim. \square

4 CPPs from exceptional polynomials of type B)

Throughout this section we assume that $n + 1 = p$. For $p = 2$, it is straightforward that there exist no exceptional polynomials of type B); hence, we assume that $p \neq 2$. We denote by $\mathbb{N}_{\mathbb{F}_q/\mathbb{F}_p}$ the norm map $\mathbb{F}_q \rightarrow \mathbb{F}_p$, $x \mapsto x^{1+p+p^2+\dots+q/p}$.

Theorem 4.1. *Assume that $(n+1)^4 < q$. The monomial $b^{-1}x^{\frac{q^n-1}{q-1}+1}$ is a CPP of \mathbb{F}_{q^n} if and only if, for some divisor r of n , one of the following cases occurs:*

i) *b is an element of $\{-\zeta_r^i \alpha \mid i \in \{0, \dots, r-1\}, \alpha^r = \zeta_{q-1}^j, \gcd(r, j) = 1\}$, or*

ii) *b is an element of*

$$\left\{ (v_0 - \lambda u_0)^{\frac{p-1}{r}} - e \mid \lambda \in \mathbb{F}_p^*, e, u_0^{p-1} \in \mathbb{F}_q^*, u_0^{\frac{(p-1)(q-1)}{r}} \neq 1, \right.$$

$$\left. v_0^{\frac{p-1}{r}} = e, \text{ord} \left(\mathbb{N}_{\mathbb{F}_q/\mathbb{F}_p} \left(\frac{u_0^{p-1}}{e^r} \right) \right) = p-1 \right\}.$$

Proof. Up to CPP-equivalence, the only indecomposable exceptional polynomials of degree p over \mathbb{F}_q are the polynomials

$$g(x) = (x + e)((x + e)^r - a)^k,$$

where r is a divisor of n and $k = n/r$, with $a, e \in \mathbb{F}_q$, $a^{\frac{q-1}{r}} \neq 1$; see [14, Theorem 8.4.14]. Hence,

$$h_g(-x) = \frac{1}{-x} \left((-x+e) ((-x+e)^r - a)^k - e (e^r - a)^k \right).$$

We distinguish a number of cases.

- $a = 0$. In this case the polynomial $g(x) = (x+e)^p$ is not good.
- $e = 0$ and $a \neq 0$. We have that $h_g(-x) = ((-x)^r - a)^k$ has r distinct roots with multiplicity k , namely $-\zeta_r^i \alpha$, where $\alpha^r = a$ and $i = 0, \dots, k-1$. They form a single orbit under the Frobenius map if and only if $x^r - a$ is irreducible over \mathbb{F}_q . By [12, Theorem 3.75], this is equivalent to require that $a = \zeta_{q-1}^j$ with $\gcd(r, j) = 1$.
- $e \neq 0$ and $a \neq 0$. Fix u_0, v_0 such that $u_0^{p-1} = a$ and $v_0^k = e$. It is straightforward to check that the set of roots of $h_g(-x)$ contains

$$R = \{ (v_0 - \lambda u_0)^k - e \mid \lambda \in \mathbb{F}_p^* \}.$$

Note that $e^r \neq a$, since $a^{\frac{q-1}{r}} \neq 1 = (e^r)^{\frac{q-1}{r}}$. We show that R actually consists of the $p-1$ distinct roots of $h_g(-x)$. Assume on the contrary that $(v_0 - \lambda u_0)^k - e = (v_0 - \lambda' u_0)^k - e$ for some $\lambda \neq \lambda'$. Then $v_0 - \lambda u_0 = \mu(v_0 - \lambda' u_0)$ for some μ with $\mu^k = 1$, and hence $v_0(1 - \mu) = u_0(\lambda - \mu\lambda')$. Since k divides $p-1$, both μ and $\mu-1$ lies in \mathbb{F}_p . As $\lambda \neq \lambda'$ we have $\mu \neq 1$ and hence $1 = (v_0/u_0)^{p-1} = e^{\frac{p-1}{k}}/a = e^r/a$, a contradiction.

In the following we prove that the elements of R are in the same orbit under the Frobenius map if and only if

$$\text{ord} \left(\mathbb{N}_{\mathbb{F}_q/\mathbb{F}_p} \left(\frac{a}{e^r} \right) \right) = p-1.$$

Let $i \in \{1, \dots, p-1\}$ be the smallest positive integer such that $((v_0 - \lambda u_0)^k - e)^{q^i} = (v_0 - \lambda u_0)^k - e$, so that the elements of R are in the same orbit under the Frobenius map if and only if $i = p-1$.

Since $u_0^{q^i} = u_0 a^{(q^i-1)/(p-1)}$ and $v_0^{q^i} = v_0 e^{(q^i-1)/k}$, the condition $(v_0 - \lambda u_0)^{kq^i} = (v_0 - \lambda u_0)^k$ holds if and only if

$$(v_0 e^{(q^i-1)/k} - \lambda u_0 a^{(q^i-1)/(p-1)})^k = (v_0 - \lambda u_0)^k,$$

which is equivalent to

$$\left(v_0 - \lambda u_0 \frac{a^{(q^i-1)/(p-1)}}{e^{(q^i-1)/k}} \right)^k = (v_0 - \lambda u_0)^k,$$

that is,

$$\left(v_0 - \lambda u_0 \frac{a^{(q^i-1)/(p-1)}}{e^{(q^i-1)/k}} \right) = \xi(v_0 - \lambda u_0),$$

where $\xi^k = 1$. Suppose $\xi \neq 1$, then

$$v_0/u_0 = \lambda \frac{\frac{a^{(q^i-1)/(p-1)}}{e^{(q^i-1)/k}} - \xi}{1 - \xi} \in \mathbb{F}_p^*,$$

and hence $(v_0/u_0)^{p-1} = 1$; this implies $a = e^{(p-1)/k} = e^r$, impossible. This means $\xi = 1$, that is

$$\frac{a^{(q^i-1)/(p-1)}}{e^{(q^i-1)/k}} = 1. \quad (1)$$

Since

$$\frac{q^i - 1}{p - 1} \equiv \frac{i(q - 1)}{p - 1} \pmod{q - 1} \quad \text{and} \quad \frac{q^i - 1}{k} \equiv \frac{i(q - 1)}{k} \pmod{q - 1},$$

Equation (1) is equivalent to

$$\frac{a^{i(q-1)/(p-1)}}{e^{i(q-1)/k}} = 1,$$

that is,

$$\left(\mathbb{N}_{\mathbb{F}_q/\mathbb{F}_p} \left(\frac{a}{e^{(p-1)/k}} \right) \right)^i = 1.$$

Therefore, $i = p - 1$ if and only if $\text{ord} \left(\mathbb{N}_{\mathbb{F}_q/\mathbb{F}_p} \left(\frac{a}{e^{(p-1)/k}} \right) \right) = p - 1$. The thesis follows. \square

5 CPPs from exceptional polynomials of type C)

In this section we deal with one of the three classes of exceptional polynomials of type C), namely the third class in [14, Theorem 8.4.12 with $e = 1$].

Proposition 5.1. *Let $p = 3$, $s = p^r > 3$, $\gcd(r, 2m) = 1$. The exceptional polynomial*

$$f_e(x) = (x + e)((x + e)^2 - a)^{(s+1)/4} \left(\frac{((x + e)^2 - a)^{(s-1)/2} + a^{(s-1)/2}}{(x + e)^2} \right)^{(s+1)/2},$$

where a is a non-square in \mathbb{F}_q^* , is not good over \mathbb{F}_q .

Proof. Following [19, Prop. 2], consider $\tau(y) = (Ey + F)/(\overline{F}y + \overline{E})$, with $E, F, \overline{E}, \overline{F} \in \mathbb{F}_{q^2}$ and $E\overline{E} - F\overline{F} = 1$. The points (x, y) of the curve with equation $\frac{f_0(x) - f_0(y)}{x - y}$ are exactly the points such that $x = \tau(y)$, where the choice of (E, F) is unique up to replacing (E, F) by $(-E, -F)$ and one of the following cases occurs:

- $F\overline{F} = -1/2$;
- $(EF\overline{E}\overline{F})^{(q-1)/2} = -1$ and $F\overline{F} \neq -1/2$;
- $(EF\overline{E}\overline{F})^{(q-1)/2} = 1$.

For $e \in \mathbb{F}_q$, a zero of $h_{f_e}(-x) = \frac{f_e(-x) - f_e(0)}{-x}$ corresponds to the point $(-x + e, e)$ of the curve defined by $\frac{f_0(x) - f_0(y)}{x - y} = 0$, that is $x = y - \tau(y)$ for some τ as described above. Since $E, F, \overline{E}, \overline{F} \in \mathbb{F}_{q^2}$, we have $(\tau(y))^{q^2} = \tau(y)$ and $x^{q^2} = x$. Therefore, the roots of $h_{f_e}(-x)$ are not in a unique orbit under the Frobenius map. \square

6 CPPs from exceptional polynomials of type D)

Throughout this section we assume that $n + 1 = p^r$ with $r > 1$. No complete classification of indecomposable exceptional polynomials of type D) is known. The following propositions deal with the cases related to linearized polynomials.

Proposition 6.1. *Let $j, k \geq 1$ and $H(x) \in \mathbb{F}_q[x]$ such that $L(x) = x^j H(x^k)$ is a linearized polynomial of degree $n + 1$. For $e \in \mathbb{F}_q$ we have that $S_e(x) = (x + e)^j H^k(x + e) - e^j H^k(e)$ is a good exceptional polynomial over \mathbb{F}_q if and only if the elements $e - (e_0 - \ell)^k$ belong to a unique orbit under the Frobenius map, where e_0 is a fixed k -th root of e and ℓ ranges over the roots of $L(x) \setminus \{0\}$.*

Proof. Following [8, Theorem 2.1] we give the factorization of the curve defined by $S_0(x^k) - S_0(y^k) = 0$. Let $N := \deg(H) = \frac{(n+1)-j}{k}$ and write

$$H(t) = \prod_{h=1}^N (t - \gamma_h),$$

where $\gamma_h \in \overline{\mathbb{F}_q}$. Then the roots of $H(t)$ and $L(x) = x^j H(x^k)$ are $\mathcal{H} = \{\gamma_h : h = 1, \dots, N\}$ and $\mathcal{L} = \{\zeta_k^i \gamma_h : i = 0, \dots, k-1, h = 1, \dots, N\} \cup \{0\}$, respectively.

Since $S_0(x^k) = (L(x))^k$, we have

$$S_0(x^k) - S_0(y^k) = (L(x))^k - (L(y))^k = \prod_{i=0}^{k-1} (L(x) - \zeta_k^i L(y)) = \prod_{i=0}^{k-1} L(x - \zeta_k^i y)$$

$$= (x^k - y^k)^j \prod_{\alpha=0}^{d-1} \prod_{\beta=0}^{d-1} \prod_{h=1}^N \left(y - \zeta_k^\alpha x - \zeta_k^\beta \gamma_h \right).$$

Consider the curve \mathcal{C}_S defined by $S_0(x) - S_0(y) = 0$. Clearly, the points (x, y) of \mathcal{C}_S satisfy $\bar{y} = \zeta_k^\alpha \bar{x} + \zeta_k^\beta \gamma_h$, where $h \in \{1, \dots, N\}$, $\alpha, \beta \in \{0, \dots, k-1\}$, $\bar{x}^k = x$, $\bar{y}^k = y$.

Now consider the polynomial $h_{S_e}(-x) = \frac{S_e(-x) - S_e(0)}{-x}$. The zeros of $h_{S_e}(-x)$ correspond to the points $(-x + e, e)$ of \mathcal{C}_S , $x \neq 0$. Fix e_0 such that $e_0^k = e$; then the zeros of $h(-x)$ are $\{e - (e_0 - \ell)^k \mid \ell \in \mathcal{L} \setminus \{0\}\}$. \square

In general, it is not easy to establish when the elements $e - (e_0 - \ell)^k$ belong to the same orbit under the Frobenius map. The following propositions provide two families of good exceptional polynomials arising from linearized polynomials.

Proposition 6.2. *Let $q = p^m$ and $L(x) = x^{p^r} - \zeta_{q-1}x \in \mathbb{F}_q[x]$. If r divides m , then $L(x)$ is good exceptional over \mathbb{F}_q .*

Proof. Let $N = p^r - 1$, and let $\eta \in \mathbb{F}_{q^N}$ be a root of $h_L(-x) = x^N - \zeta_{q-1}$. Then the roots of $h_L(-x)$ are $\{\lambda\eta \mid \lambda \in \mathbb{F}_{p^r}^*\}$. The hypothesis $r \mid m$ is equivalent to require that N divides $(q-1)$, and this implies that $N(q-1) \mid q^N - 1$. Hence we can choose $\eta = \omega^{\frac{q^N-1}{N(q-1)}}$, where ω is a primitive element of \mathbb{F}_{q^N} . The thesis is proved by showing that η is not an element of any proper subfield of \mathbb{F}_{q^N} . Suppose that $\eta \in \mathbb{F}_{q^k}$ with $k \mid N$. Then $\omega^{\frac{q^N-1}{N(q-1)}(q^k-1)} = 1$, that is $N \mid \frac{q^k-1}{q-1}$; since $q \equiv 1 \pmod{N}$, this is equivalent to $N \mid k$, and hence to $N = k$. \square

Proposition 6.3. *If $\gcd(m, p^r - 1)$ is a divisor of r , then there exists a linearized polynomial $L(x) \in \mathbb{F}_q[x]$ of degree p^r which is good exceptional over \mathbb{F}_q .*

Proof. Let $\epsilon = \gcd(m, p^r - 1)$ and $\ell(x) \in \mathbb{F}_q[x]$ be a primitive polynomial of degree r/ϵ over \mathbb{F}_{p^ϵ} , so that $\ell(x)$ is irreducible over \mathbb{F}_{p^ϵ} and has order $p^r - 1$. Let $L(x) \in \mathbb{F}_q[x]$ be the linearized p^ϵ -associate of $\ell(x)$. Then, by [12, Theorem 3.63], the polynomial $L(x)/x$ is irreducible over \mathbb{F}_{p^ϵ} . Let α be a non-zero root of $L(x)$. Then the field extension $\mathbb{F}_{p^\epsilon}(\alpha) : \mathbb{F}_{p^\epsilon}$ has degree $p^r - 1$, while the extension $\mathbb{F}_q : \mathbb{F}_{p^\epsilon}$ has degree m/ϵ . The field $\mathbb{F}_q(\alpha)$ is the compositum of \mathbb{F}_q and $\mathbb{F}_{p^\epsilon}(\alpha)$; since $\gcd(m/\epsilon, p^r - 1) = 1$, we have that $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = p^r - 1$. Then $L(x)/x = h_L(-x)$ is irreducible over \mathbb{F}_q , and the thesis follows. \square

7 The cases $n + 1 = 8$ and $n + 1 = 9$

The aim of this section is to study the cases $n + 1 = 8$ (with $p = 2$) and $n + 1 = 9$ (with $p = 3$). Since no complete classification of exceptional polynomials is known, we study the

existence of good exceptional polynomials via algebraic curves associated to a PP. In fact, a polynomial $f(x)$ is a PP of \mathbb{F}_q if and only if the algebraic curve \mathcal{C}_f of degree n with equation

$$\frac{f(x) - f(y)}{x - y} = 0$$

has no \mathbb{F}_q -rational points off the ideal line and the line $x = y$. For q large enough with respect to the degree of $f(x)$, by the Hasse-Weil bound this is only possible when \mathcal{C}_f splits into components not defined over \mathbb{F}_q ; see for instance [1]. On the other hand, if \mathcal{C}_f has no absolutely irreducible component defined over \mathbb{F}_q , with the only possible exception of the line $x = y$, then $f(x)$ is a permutation polynomial over an infinite number of extensions of \mathbb{F}_q , that is $f(x)$ is exceptional over \mathbb{F}_q ; see [7] and [14, Chapter 8.4].

7.1 $n + 1 = 8, p = 2$

Proposition 7.1. *Let $q = 2^m$, $n + 1 = 8$. The polynomial $f(x) = x^8 + \sum_{i=1}^7 A_i x^{8-i} \in \mathbb{F}_q[x]$ is exceptional over \mathbb{F}_q if and only if $A_1 = A_2 = A_3 = A_5 = 0$ and the polynomial $g(x) = x^7 + A_4 x^3 + A_6 x + A_7$ has no roots in \mathbb{F}_q^* . Also $f(x)$ is good exceptional if and only if $g(x)$ is irreducible over \mathbb{F}_q .*

Proof. The equation of the curve \mathcal{C}_f reads

$$(x + y)^7 + A_1(x^6 + x^5 y + x^4 y^2 + x^3 y^3 + x^2 y^4 + x y^5 + y^6) + A_2(x^5 + x^4 y + x^3 y^2 + x^2 y^3 + x y^4 + y^5) + A_3(x^4 + x^3 y + x^2 y^2 + x y^3 + y^4) + A_4(x + y)^3 + A_5(x^2 + x y + y^2) + A_6(x + y) + A_7 = 0.$$

Applying the Frobenius automorphism $t \mapsto t^q$ to the factors of \mathcal{C}_f it is easy to conclude that if the curve \mathcal{C}_f does not have absolutely irreducible components defined over \mathbb{F}_q , then the curve contains either two conics and three lines or seven lines. The unique ideal point of \mathcal{C}_f is $(1 : 1 : 0)$. A line ℓ that is a component of the curve \mathcal{C}_f has equation $\ell : y = x + \alpha$ and

$$\begin{cases} A_1 = 0 \\ A_2 \alpha + A_3 = 0 \\ A_2 \alpha^3 + A_5 = 0 \\ A_3 \alpha^2 + A_5 = 0 \\ \alpha^7 + A_2 \alpha^5 + A_3 \alpha^4 + A_4 \alpha^3 + A_5 \alpha^2 + A_6 \alpha + A_7 = 0. \end{cases}$$

If the line ℓ is not defined over \mathbb{F}_q then $\alpha \in \overline{\mathbb{F}_q} \setminus \mathbb{F}_q$; this yields $A_2 = A_3 = A_5 = 0$, and the last equality becomes $\alpha^7 + A_4 \alpha^3 + A_6 \alpha + A_7 = 0$. It is easily seen that if $A_2 = A_3 = A_5 = 0$ then the curve \mathcal{C}_f contains the seven lines $y + x + \alpha_i = 0$, $i = 1, \dots, 7$, where $\alpha_i^7 + A_4 \alpha_i^3 + A_6 \alpha_i + A_7 = 0$, and therefore \mathcal{C}_f cannot split in two conics and three lines.

Thus, the only open case occurs when \mathcal{C}_f splits in seven lines either not defined over \mathbb{F}_q or equal to $x - y = 0$.

Therefore $f(x)$ is exceptional if and only if $T^7 + A_4T^3 + A_6T + A_7$ has no roots in \mathbb{F}_q and it is good exceptional if and only if $T^7 + A_4T^3 + A_6T + A_7$ is irreducible over \mathbb{F}_q since all the roots must be in the same orbit. \square

Corollary 7.2. *Let $q = 2^m$, $n + 1 = 8$ and suppose 3 divides m . The polynomial $x^8 + A_7x$ is the only good exceptional polynomial over \mathbb{F}_q .*

Proof. Since 3 divides m we have that $\zeta_7 \in \mathbb{F}_q$. From Cyclic extensions theory, $T^7 + A_4T^3 + A_6T + A_7$ is irreducible over \mathbb{F}_q if and only if $A_4 = A_6 = 0$. The thesis follows from Proposition 7.1. \square

Remark 7.3. *The exceptional polynomials of Proposition 7.1 are linearized, and hence described in [14, Prop. 8.4.15]. Also, Proposition 7.1 confirms the conjecture [14, Remark 8.4.18] for the special case $n + 1 = 8$.*

Corollary 7.4. *Assume that $q = 2^r > 8^4$. The monomial $b^{-1}x^{\frac{q^7-1}{q-1}+1}$ is a CPP of \mathbb{F}_{q^8} if and only if b is, up to a scalar multiple in \mathbb{F}_q^* , a root of some $F(x) = x^7 + \alpha x^3 + \beta x + \gamma \in \mathbb{F}_q[x]$, irreducible over \mathbb{F}_q .*

7.2 $n + 1 = 9$, $p = 3$

Proposition 7.5. *Let $q = 3^h$. The polynomial*

$$F(x) = x^9 + A_1x^8 + A_2x^7 + A_3x^6 + A_4x^5 + A_5x^4 + A_6x^3 + A_7x^2 + A_8x$$

is exceptional over \mathbb{F}_q if and only if one of the following cases occurs.

i)

$$F(x) = x^9 + A_3x^6 + A_6x^3 \tag{2}$$

and $T^6 + A_3T^3 + A_6 \in \mathbb{F}_q[T]$ has no roots in \mathbb{F}_q^ ;*

ii)

$$F(x) = x^9 + A_6x^3 + A_8x \tag{3}$$

and $T^8 + A_6T^2 + A_8 \in \mathbb{F}_q[T]$ has no roots in \mathbb{F}_q^ ;*

iii)

$$\begin{aligned} F(x) = x^9 + A_3x^6 + A_4x^5 + A_5x^4 + & \left(A_3^2 + A_3 \frac{A_5^3}{A_4^3} + \frac{A_5^2}{A_4} \right) x^3 \\ & + \left(2A_3A_4 + 2\frac{A_5^3}{A_4^2} \right) x^2 + \left(2A_3A_5 + A_4^2 + 2\frac{A_5^4}{A_4^3} \right) x, \end{aligned} \tag{4}$$

where

(a) $A_4 \neq 0$,

(b) the polynomial $T^4 + 2A_3T + 2A_4 \in \mathbb{F}_q[T]$ has no roots in \mathbb{F}_q ;

iv)

$$F(x) = x^9 + A_2x^7 + A_3x^6 + A_5x^4 + \left(A_2^3 + \frac{A_3A_5}{A_2}\right)x^3 + \left(2A_2A_5 + 2\frac{A_3^3}{A_2}\right)x^2 + \left(A_2^4 + A_3A_5 + \frac{A_5^2}{A_2} + \frac{A_3^4}{A_2^2}\right)x, \quad (5)$$

where $2A_2$ is not a square in \mathbb{F}_q .

Proof. The curve \mathcal{C}_f associated to the polynomial $F(x) = x^9 + \sum_{i=1}^8 A_{8-i}x^i$ is

$$\sum_{i=0}^8 A_{8-i} \frac{x^{i+1} - y^{i+1}}{x - y} = 0,$$

where $A_i \in \mathbb{F}_q$, $i = 1, \dots, 8$, $A_0 = 1$, and $A_8 \neq 0$.

- Suppose that \mathcal{C}_f contains a line ℓ with equation $\ell : y = x + \alpha$, where $\alpha = 0$ or $\alpha \notin \mathbb{F}_q$. Then α satisfies:

$$\begin{cases} 2A_1 = 0 \\ 2\alpha A_1 + A_2 = 0 \\ 2\alpha^2 A_1 = 0 \\ \alpha^3 A_1 + 2\alpha^2 A_2 + A_4 = 0 \\ 2\alpha^4 A_1 + 2\alpha^3 A_2 + 2\alpha^2 A_3 + \alpha A_4 + A_5 = 0 \\ \alpha^5 A_1 + \alpha^2 A_4 = 0 \\ 2\alpha^6 A_1 + \alpha^8 A_2 + \alpha^3 A_4 + \alpha^2 A_5 + 2A_7 = 0 \\ \alpha^8 A_0 + \alpha^7 A_1 + \alpha^6 A_2 + \alpha^5 A_3 + \alpha^4 A_4 + \alpha^3 A_5 + \alpha^2 A_6 + \alpha A_7 + A_8 = 0 \end{cases}.$$

This implies $A_1 = A_2 = 0$. We distinguish two cases.

- $\alpha = 0$. Then $A_4 = A_5 = A_7 = A_8 = 0$. The curve becomes

$$(x - y)^2((x - y)^6 + A_3(x - y)^3 + A_6) = 0.$$

We have to require that the polynomial $T^6 + A_3T^3 + A_6$ has no roots in \mathbb{F}_q^* .

- $\alpha \neq 0$. Then $A_4 = 0$. The conditions above read

$$A_5\alpha^2 + 2A_7 = 0, \quad \alpha^8 + A_3\alpha^5 + A_5\alpha^3 + A_6\alpha^2 + A_7\alpha + A_8 = 0, \quad 2A_3\alpha^2 + A_5 = 0.$$

If $A_5 = 0$ then $A_3 = A_7 = 0$ and $\alpha^8 + A_6\alpha^2 + A_8 = 0$ and the curve splits in 8 lines. They are not defined over \mathbb{F}_q or equal to $x - y = 0$ if and only if the polynomial $T^8 + A_6T^2 + A_8 = 0$ has no roots in \mathbb{F}_q^* .

If $A_3 = 0$ then $A_5 = A_7 = 0$ and $\alpha^8 + A_6\alpha^2 + A_8 = 0$, as above.

Suppose now $A_3, A_5 \neq 0$. Then $A_5 = A_3\alpha^2$, $A_7 = A_5^2/A_3$, and $A_8 = 2A_5A_6/A_3 + 2A_5^4/A_3^4$. Since $\alpha^2 = A_5/A_3$, we have that A_5/A_3 is not a square in \mathbb{F}_q , otherwise the lines $y = x + \xi_1$ and $y = x + \xi_2$, where $\xi_i^2 = A_5/A_3$, are \mathbb{F}_q -rational lines and the polynomial $F(x)$ is not exceptional. Let $a_3, a_5 \in \mathbb{F}_{q^2}$ be such that $a_3^2 = A_3$ and $a_5^2 = A_5$. In this case the curve splits in

$$(a_3x - a_3y + a_5)(a_3x - a_3y - a_5) \cdot$$

$$(a_3^6(x-y)^6 + a_3^4a_5^2(x-y)^4 + a_3^8(x+y)^3 + a_3^2a_5^4(x-y)^2 - a_3^6a_5^2(x+y) + a_3^6A_6 + a_5^6) = 0.$$

Since the sextic is defined over \mathbb{F}_q , it must split either in three conics or in two cubics. In the first case it is easily seen that all of them must be fixed by ψ .

If a conic of equation $(x - y)^2 + \alpha(x + y) + \beta = 0$ is contained in the sextic then in particular $A_3^2 = \alpha^3$ from which we get $a_3^{32}a_5^{12} = 0$, impossible.

Suppose now that the sextic splits in two cubics.

If they are fixed by ψ then they have equations

$$(x - y)^3 + \alpha_1x^2 + \alpha_2xy + \alpha_1y^2 + \beta_1x + \beta_1y + \gamma_1 = 0$$

and

$$(x - y)^3 + \alpha_3x^2 + \alpha_4xy + \alpha_3y^2 + \beta_2x + \beta_2y + \gamma_2 = 0.$$

Then in particular $\alpha_4 = \alpha_3 = -\alpha_1$, $\alpha_2 = \alpha_1$. If $\alpha_1 = 0$ then $a_3^2 = \gamma_1 + \gamma_2$ and $a_3^2 = -\gamma_1 - \gamma_2$, which imply $a_3 = 0$, impossible. If $\alpha_1 \neq 0$ then $\beta_1 = \beta_2$ and again $a_3^2 = \gamma_1 + \gamma_2$ and $a_3^2 = -\gamma_1 - \gamma_2$, which imply $a_3 = 0$, impossible.

If they are switched by ψ then they have equations

$$(x - y)^3 + \alpha_1x^2 + \alpha_2xy + \alpha_3y^2 + \beta_1x + \beta_2y + \gamma_1 = 0$$

and

$$\lambda((y - x)^3 + \alpha_3x^2 + \alpha_2xy + \alpha_1y^2 + \beta_2x + \beta_1y + \gamma_1) = 0.$$

Then in particular $\lambda = -a_3^6$, $\alpha_3 = \alpha_1$. If $\alpha_2 = -\alpha_1$, then $a_3^2\alpha_1^2 + a_3^2\beta_1 - a_3^2\beta_2 - a_5^2 = 0$ and $\alpha_1 = 0$, which implies $a_3 = 0$, impossible. If $\alpha_2 = \alpha_1$, then $\alpha_1(\beta_1 + \beta_2) = 0$. In both the cases $a_3 = 0$, impossible.

- Suppose that \mathcal{C}_f splits in four absolutely irreducible conics. There are three distinct possibilities, depending on the number of components fixed by ψ .

1. All the conics are fixed by ψ . In this case the four conics are defined by

$$\mathcal{C}_i : (x - y)^2 + \alpha_i(x + y) + \beta_i = 0, \quad (6)$$

for $i = 1, 2, 3, 4$. This gives immediately $A_1 = A_2 = 0$.

The condition $A_4 = 0$ implies $A_5 = A_7 = 0$ and $A_3A_8 = 0$, that is the polynomial is either of type (2) or (3).

Suppose $A_4 \neq 0$. Then, by direct computation, $A_6 = A_3^2 + A_3A_5^3/A_4^3 + A_5^2/A_4$, $A_7 = 2A_3A_4 + 2A_5^3/A_4^2$, $A_8 = 2A_3A_5 + A_4^2 + 2A_5^4/A_4^3$; also, the α_i 's are roots of $\ell_1(x) = x^4 + 2A_3x + 2A_4$, and $\beta_i = \alpha_i^2 + A_5/A_4\alpha_i$. On the other hand if all these conditions are satisfied then the curve splits in the four conics defined in (6). Finally, the four conics are not defined over \mathbb{F}_q if and only if the polynomial $T^4 + 2A_3T + 2A_4$ has no roots in \mathbb{F}_q .

2. Two conics are fixed by ψ and two are switched. We can assume

$$\begin{aligned} \mathcal{C}_1 : (x - y)^2 + \alpha_1(x + y) + \beta_1 = 0, \quad \mathcal{C}_2 : (x - y)^2 + \alpha_2(x + y) + \beta_2 = 0, \\ \mathcal{C}_3 : (x - y)^2 + \alpha_3x + \alpha_4y + \beta_3 = 0, \quad \mathcal{C}_4 : (x - y)^2 + \alpha_4x + \alpha_3y + \beta_3 = 0. \end{aligned}$$

By direct computation, we get immediately $A_1 = A_2 = A_4 = A_5 = A_7 = 0$ and $A_3A_8 = 0$, and hence $F(x)$ is of type (2) or (3).

3. No conic is fixed by ψ . We can assume

$$\begin{aligned} \mathcal{C}_1 : (x - y)^2 + \alpha_1x + \alpha_2y + \beta_1 = 0, \quad \mathcal{C}_2 : (x - y)^2 + \alpha_2x + \alpha_1y + \beta_1 = 0, \\ \mathcal{C}_3 : (x - y)^2 + \alpha_3x + \alpha_4y + \beta_2 = 0, \quad \mathcal{C}_4 : (x - y)^2 + \alpha_4x + \alpha_3y + \beta_2 = 0. \end{aligned}$$

Also in this case we get $A_1 = A_2 = A_4 = A_5 = A_7 = 0$ and $A_3A_8 = 0$, and hence $F(x)$ is of type (2) or (3).

- Suppose that \mathcal{C}_f splits in two absolutely irreducible quartics \mathcal{Q}_1 and \mathcal{Q}_2 . The automorphism ψ can either switch or fix the two components.

In the former case, \mathcal{Q}_1 and \mathcal{Q}_2 have the form

$$\begin{aligned} \mathcal{Q}_1 : (x - y)^4 + \alpha_1x^3 + \alpha_2x^2y + \alpha_3xy^2 + \alpha_4y^3 + \beta_1x^2 + \beta_2xy + \beta_3y^2 + \gamma_1x + \gamma_2y + \delta = 0, \\ \mathcal{Q}_2 : (x - y)^4 + \alpha_4x^3 + \alpha_3x^2y + \alpha_2xy^2 + \alpha_1y^3 + \beta_3x^2 + \beta_2xy + \beta_1y^2 + \gamma_2x + \gamma_1y + \delta = 0. \end{aligned}$$

We get $A_1 = A_2 = A_3 = A_4 = A_5 = A_7 = 0$; hence, we have case (3).

In the latter case, \mathcal{Q}_1 and \mathcal{Q}_2 have the form

$$\begin{aligned} \mathcal{Q}_1 : (x - y)^4 + \alpha_1x^3 + \alpha_2x^2y + \alpha_2xy^2 + \alpha_1y^3 + \beta_1x^2 + \beta_2xy + \beta_1y^2 + \gamma_1(x + y) + \delta_1 = 0, \\ \mathcal{Q}_2 : (x - y)^4 + \alpha_3x^3 + \alpha_4x^2y + \alpha_4xy^2 + \alpha_3y^3 + \beta_3x^2 + \beta_4xy + \beta_3y^2 + \gamma_2(x + y) + \delta_2 = 0. \end{aligned}$$

Since $A_1 = 0$, we obtain $A_2A_4 = 0$.

- Suppose $A_2 = 0$ and $A_4 \neq 0$. Then $A_6 = A_3^2 + A_3A_5^3/A_4^3 + A_5^2/A_4$, $A_7 = 2A_3A_4 + 2A_5^3/A_4^2$, $A_8 = 2A_3A_5 + A_4^2 + A_5^4/A_4^3$ and we have case (4).
- Suppose now $A_2 \neq 0$ and $A_4 = 0$. Then $A_6 = A_2^3 + A_3A_5/A_2$, $A_7 = 2A_2A_5 + 2A_3^3/A_2$, $A_8 = A_2^4 + A_3A_5 + A_5^2/A_2 + A_3^4/A_2^2$. Also, $\alpha_1^2 = 2A_2$, $\alpha_2 = \alpha_3 = -\alpha_4 = -\alpha_1$, $\beta_1 = -\beta_3 = 2A_3/\alpha_1$, $\beta_2 = -A_3/\alpha_1 - \alpha_1^2$, $\beta_4 = A_3/\alpha_1 - \alpha_1^2$, $\gamma_1 = A_3 + \alpha_1^3$, $\gamma_2 = A_3 - \alpha_1^3$, $\delta_1 = A_3\alpha_1 + A_3^2/A_2 + 2A_5\alpha_1/A_2 + 2\alpha_1^6/A_2$, $\delta_2 = -A_3\alpha_1 + A_3^2/A_2 + A_5\alpha_1/A_2 + 2\alpha_1^6/A_2$. Note that $\alpha_i, \beta_i, \gamma_i, \delta_i$ are not defined over \mathbb{F}_q if and only if $2A_2$ is not a square in \mathbb{F}_q . The quartics \mathcal{Q}_1 and \mathcal{Q}_2 read

$$\begin{aligned} & (x - y)^4 + \alpha_1 x^3 + 2\alpha_1 x^2 y + 2\alpha_1 x y^2 + \alpha_1 y^3 + 2A_3/\alpha_1 x^2 + 2(A_3/\alpha_1 + \alpha_1^2)xy \\ & + 2A_3/\alpha_1 y^2 + (A_3 + \alpha_1^3)(x + y) + A_3\alpha_1 + A_3^2/A_2 + 2A_5\alpha_1/A_2 + 2\alpha_1^6/A_2 = 0, \\ & (x - y)^4 + 2\alpha_1 x^3 + \alpha_1 x^2 y + \alpha_1 x y^2 + 2\alpha_1 y^3 + A_3/\alpha_1 x^2 + (A_3/\alpha_1 + 2\alpha_1^2)xy \\ & + A_3/\alpha_1 y^2 + (A_3 + 2\alpha_1^3)(x + y) + 2A_3\alpha_1 + A_3^2/A_2 + A_5\alpha_1/A_2 + 2\alpha_1^6/A_2 = 0, \end{aligned}$$

and \mathcal{Q}_1 and \mathcal{Q}_2 are switched by the Frobenius map.

- Finally, $A_2 = A_4 = 0$ implies $A_5 = A_7 = 0$ and $A_3A_8 = 0$. As above, this gives types (2) or (3).

□

Remark 7.6. By direct computation, the exceptional polynomials of Proposition 7.5 are equivalent to exceptional polynomials described in [14, Prop. 8.4.15].

In fact, if $F(x)$ satisfies Case i) or ii), then $F(x)$ is a linearized polynomial.

If $F(x)$ satisfies Case iii), then $F(x) = L_1 \circ S \circ L_2(x)$, where $L_1(x)$ and $L_2(x)$ are linear, and $S(x) \in \mathbb{F}_q[x]$ has the form $x(a_2x^4 + a_1x + a_0)^2$.

If $F(x)$ satisfies Case iv), then $F(x) = L_1 \circ S \circ L_2(x)$, where $L_1(x)$ and $L_2(x)$ are linear, and $S(x) \in \mathbb{F}_q[x]$ has the form $S(x) = x(a_2x^4 + a_1x + a_0)^2$ when $A_2^2A_5 + A_3^3 \neq 0$, or $S(x) = x(a_2x^2 + a_0)^4$ when $A_2^2A_5 + A_3^3 = 0$.

This confirms the conjecture [14, Remark 8.4.18] for the special case $n + 1 = 9$.

Proposition 7.7. Let $q = 3^h$. The polynomial

$$F(x) = x^9 + A_1x^8 + A_2x^7 + A_3x^6 + A_4x^5 + A_5x^4 + A_6x^3 + A_7x^2 + A_8x$$

is good exceptional over \mathbb{F}_q if and only if one of the following cases occurs.

i)

$$F(x) = x^9 + A_6x^3 + A_8x$$

and $x^8 + A_6x^2 + A_8$ is irreducible over \mathbb{F}_q ;

ii)

$$F(x) = x^9 + A_3x^6 + A_4x^5 + A_5x^4 + \left(A_3^2 + A_3\frac{A_5^3}{A_4^3} + \frac{A_5^2}{A_4}\right)x^3 \\ + \left(2A_3A_4 + 2\frac{A_5^3}{A_4^2}\right)x^2 + \left(2A_3A_5 + A_4^2 + 2\frac{A_5^4}{A_4^3}\right)x,$$

where

(a) $A_4 \neq 0$,

(b) the polynomial $x^8 + 2A_3x^2 + 2A_4 \in \mathbb{F}_q[x]$ has no roots in \mathbb{F}_{q^4} ;

iii)

$$F(x) = x^9 + A_2x^7 + A_3x^6 + A_5x^4 + \left(A_2^3 + \frac{A_3A_5}{A_2}\right)x^3 + \\ \left(2A_2A_5 + 2\frac{A_3^3}{A_2}\right)x^2 + \left(A_2^4 + A_3A_5 + \frac{A_5^2}{A_2} + \frac{A_3^4}{A_2^2}\right)x,$$

where

(a) $2A_2$ is not a square in \mathbb{F}_q ,

(b) $h(-x) = (x^4 + 2\alpha x^3 + 2A_3/\alpha x^2 + 2(A_3 + 2\alpha A_2)x + A_3\alpha + A_3^2/A_2 + 2A_5\alpha/A_2 + A_2^2)(x^4 + \alpha x^3 + A_3/\alpha x^2 + 2(A_3 + \alpha A_2)x + 2A_3\alpha + A_3^2/A_2 + A_5\alpha/A_2 + A_2^2)$, where $\alpha^2 = 2A_2$, is irreducible over \mathbb{F}_q .

Proof. We use the classification of exceptional polynomials of degree 9 given in Proposition 7.5.

- Let $F(x)$ be as in Case i) of Proposition 7.5. Then $A_8 = 0$; hence, $F(x)$ is not good.
- Let $F(x)$ be as in Case ii) of Proposition 7.5. Then $h_F(-x) = x^8 + A_6x^2 + A_8$; since $h_F(-x)$ cannot be a square in $\mathbb{F}_q[x]$, we have that $F(x)$ is good if and only if $h_F(-x)$ is irreducible over \mathbb{F}_q .
- Let $F(x)$ be as in Case iii) of Proposition 7.5. The factors of $h_F(-x)$ are $x^2 - \alpha_i x + \beta_i$, $i = 1, \dots, 4$, where the α_i 's are roots of $\ell_1(x) = x^4 + 2A_3x + 2A_4$ and $\beta_i = \alpha_i^2 + A_5/A_4\alpha_i$; hence, $\ell_1(x)$ must be irreducible over \mathbb{F}_q in order for $F(x)$ to be good. Also, the roots of $h(-x)$ are $-\alpha_i \pm \sqrt{-A_5/A_4\alpha_i}$. Since $-A_5/A_4$ is an element of \mathbb{F}_q and hence a square in \mathbb{F}_{q^4} , the roots of $h(-x)$ are in the same orbit under the Frobenius map if and only if α_i is not a square in \mathbb{F}_{q^4} , that is the polynomial $x^8 + 2A_3x^2 + 2A_4 \in \mathbb{F}_q[x]$ has no roots in \mathbb{F}_{q^4} .

- Let $F(x)$ be as in Case *iv*) of Proposition 7.5. The polynomial $h_F(-x)$ reads

$$(x^4 + 2\alpha x^3 + 2A_3/\alpha x^2 + 2(A_3 + 2\alpha A_2)x + A_3\alpha + A_3^2/A_2 + 2A_5\alpha/A_2 + A_2^2) \cdot \\ \cdot (x^4 + \alpha x^3 + A_3/\alpha x^2 + 2(A_3 + \alpha A_2)x + 2A_3\alpha + A_3^2/A_2 + A_5\alpha/A_2 + A_2^2),$$

where $\alpha^2 = 2A_2$. Hence, the roots of $h_F(-x)$ are in a unique orbit under the Frobenius map if and only if $h_F(-x)$ is irreducible over \mathbb{F}_q .

□

Remark 7.8. We give two families of good exceptional polynomials arising from Proposition 7.7. Let $q = 3^h$ with h even, and η be an odd number; by [12, Theorem 3.75], the polynomial $x^8 + 2\zeta_{q-1}^\eta \in \mathbb{F}_q[x]$ is irreducible over \mathbb{F}_q . Therefore, by Case *i*) in Proposition 7.7, the polynomial $F(x) = x^9 + 2\zeta_{q-1}^\eta x$ is good exceptional over \mathbb{F}_q . Also, by Case *ii*) in Proposition 7.7, the polynomial

$$F(x) = x^9 + \zeta_{q-1}^\eta x^5 + ax^4 + \frac{a^2}{\zeta_{q-1}^\eta} x^3 + 2\frac{a^3}{\zeta_{q-1}^{2\eta}} x^2 + \left(\zeta_{q-1}^{2\eta} + 2\frac{a^4}{\zeta_{q-1}^{3\eta}} \right) x$$

is good exceptional over \mathbb{F}_q , for any $a \in \mathbb{F}_q$.

Corollary 7.9. Assume that $q = 3^r > 8^4$. The monomial $b^{-1}x^{\frac{q^8-1}{q-1}+1}$ is a CPP of \mathbb{F}_{q^8} if and only if b is, up to a scalar multiple in \mathbb{F}_q^* , a root of some $(F(-x+e) - F(e))/(-x) \in \mathbb{F}_q[x]$, where $e \in \mathbb{F}_q$ and $F(x) \in \mathbb{F}_q[x]$ satisfies Case *i*), *ii*), or *iii*) in Proposition 7.7.

8 Acknowledgements

The research of D. Bartoli, M. Giulietti, and G. Zini was partially supported by Ministry for Education, University and Research of Italy (MIUR) (Project PRIN 2012 “Geometrie di Galois e strutture di incidenza” - Prot. N. 2012XZE22K_005) and by the Italian National Group for Algebraic and Geometric Structures and their Applications (GNSAGA - INdAM).

The research of L. Quoos was partially supported by CNPq – Proc. 200434/2015-2. This work was done while L. Quoos was enjoying a sabbatical at the Università degli Studi di Perugia.

References

- [1] D. Bartoli, M. Giulietti, G. Zini, *On monomial complete permutation polynomials*, Finite Fields Appl. **41** (3) (2016) 132–158.

- [2] L.A. Bassalygo, V.A. Zinoviev, *On one class of permutation polynomials over finite fields of characteristic two*, Mosc. Math. J. **15** (4) (2015) 703–713.
- [3] L.A. Bassalygo, V.A. Zinoviev, *Permutation and complete permutation polynomials*, Finite Fields Appl. **33** (2015) 198–211.
- [4] M. Bhargava, M. E. Zieve, *Factoring Dickson Polynomials over Finite Fields*, Finite Fields Appl. **5** (1999) 103–111.
- [5] S. Bhattacharya, S. Sarkar, *On some permutation binomials and trinomials over \mathbb{F}_{2^n}* , Des. Codes Cryptogr. **82** (2017) 149–160.
- [6] Y. Laigle-Chapuy, *Permutation polynomials and applications to coding theory*, Finite Fields Appl. **13** (1) (2007) 58–70.
- [7] S.D. Cohen, *The distribution of polynomials over finite fields*, Acta Arith. **17** (1970) 255–271.
- [8] S.D. Cohen, *Exceptional polynomials and the reducibility of substitution polynomials*, L’Enseignement Mathématique **36** (1990) 53–65.
- [9] S.D. Cohen, R.W. Matthews, *Exceptional polynomials over finite fields*, Finite Fields Appl. **1** (1995) 261–277.
- [10] R.M. Guralnick, M.E. Zieve, *Polynomials with $\text{PSL}(2)$ monodromy*, Annals of Math. **172** (2010) 1321–1365.
- [11] G.L. Mullen, H. Niederreiter, *Dickson polynomials over finite fields and complete mappings*, Can. Math. Bull. **30** (1) (1987) 19–27.
- [12] R. Lidl, H. Niederreiter, *Introduction to Finite Fields and their Applications*, Cambridge University Press, 1986.
- [13] J. Ma, T. Zhang, T. Feng, G. Ge, *New results on permutation polynomials over finite fields*, arXiv:1506.05525.
- [14] G.L. Mullen, D. Panario, *Handbook of Finite Fields*, Chapman and Hall, 2013.
- [15] P. Stanica, S. Gangopadhyay, A. Chaturvedi, A.K. Gangopadhyay, S. Maitra, *Investigations on bent and negabent functions via the nega-Hadamard transform*, IEEE Trans. Inf. Theory **58** (6) (2012) 4064–4072.

- [16] G. Wu, N. Li, T. Helleseeth, Y. Zhang, *Some classes of monomial complete permutation polynomials over finite fields of characteristic two*, Finite Fields Appl. **28** (2014) 148–165.
- [17] G. Wu, N. Li, T. Helleseeth, Y. Zhang, *Some classes of complete permutation polynomials over \mathbb{F}_q* , Sci. China Math. **58** (10) (2015) 2081–2094.
- [18] G. Wu, N. Li, T. Helleseeth, Y. Zhang, *More Classes of Complete Permutation Polynomials over \mathbb{F}_q* , arXiv:1312.4716.
- [19] M. Zieve, *Bivariate factorizations via Galois theory, with application to exceptional polynomials*, J. Algebra **210** (1998) 670–689.
- [20] Y. Zhou, L. Qu, *Constructions of negabent functions over finite fields*, Cryptography and Communications (2015) 1–16.

Daniele Bartoli and Massimo Giulietti are with
 Dipartimento di Matematica e Informatica
 Università degli Studi di Perugia
 Via Vanvitelli, 1 - 06123 Perugia - Italy
emails: daniele.bartoli,massimo.giulietti@unipg.it

Giovanni Zini is with
 Dipartimento di Matematica e Informatica “Ulisse Dini”
 Università degli Studi di Firenze
 Viale Morgagni, 67/A - 50134 Firenze - Italy
email: gzini@math.unifi.it

Luciane Quoos is with
 Instituto de Matemática
 Universidade Federal do Rio de Janeiro
 Rio de Janeiro 21941-909 - Brazil
email: luciane@im.ufrj.br.